Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

e-Authentication Risk and Requirements Assessment

Guide v0.996 BETA

Networked Systems Survivability Program

August 2003

Table of Contents

Acknowledgements

e-RA Overview

e-RA definition

e-RA is the e-Authentication Risk and Requirements Assessment approach. It is a risk-based technique to elicit authentication requirements for electronic transactions.

Its purpose is to guide users in selecting an appropriate level of authentication to resist threats to their data, users, and organizations that could result from unauthorized use of system transactions.

Risk-based approach

The e-RA approach emphasizes the development of authentication requirements based on risk. It helps you to identify and assess the risks that can result from unauthorized use of transactions. This helps you identify your true authentication needs and match them to appropriate technical solutions.

Viewing authentication purely as a technology issue sometimes causes the deployment of common technology-centric approaches (such as a public key infrastructure) that may not align properly with your authentication requirements. Technology-centric approaches can be

- more costly than you need

- difficult to implement, manage, and maintain

- a barrier to your intended customers

Using risk to drive the identification of authentication requirements allows you to find and deploy a technical solution that is neither too ineffective nor extensive for your needs.

Improper authentication of users can result in direct and dire consequences to an initiative. The e-RA approach prompts you to look at your transactions as though **no authentication controls have been implemented.** In this abstract case, e-RA helps you to identify the risks to which the initiative, its users, and its business partners would be subjected if unauthorized use of transactions occurs. By understanding these risks, you are better able to develop authentication requirements that are based on avoiding the risks unique to your initiative, rather than accepting a canned technical solution.

Improper authentication can occur in many ways, including

- a lack of authentication controls

- authentication controls that are inappropriate or weak

- assignment of an inappropriate level of authentication to a user

- poor implementation of authentication controls

- corruption or compromise of authentication controls

e-RA is not, however, a risk assessment methodology for assessing all these types of authentication risks. e-RA is focused on requirements elicitation, and is not intended as a risk assessment of the operational management of an authentication infrastructure. An operational assessment would be better performed as part of a regular risk-based security assessment.

Authentication levels

Authentication is a way to ensure that users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.

Origin of authentication levels

For simplicity and consistency, authentication levels are used in e-RA to describe the various degrees of proving the identity of users. The developers of the e-RA approach have included authentication levels that are roughly based on UK standards and consistent with OMB standards. However, users of e-RA can substitute any authentication schema that works for them. The basic e-RA process is flexible and can be matched with a variety of authentication levels.

Purpose of authentication levels

In e-RA, the authentication levels have two primary purposes:

- to define the characteristics of authentication that a transaction would need to deploy to prevent risks of unauthorized use from being realized

- to provide a foundation for the development of detailed authentication requirements for a set of transactions that can be translated into technical requirements for implementation

Note that the levels do not represent any particular authentication requirements or technical solutions. In the e-RA approach it is important to assign an authentication level to a transaction based on the risks of unauthorized use that have been identified. The authentication level can then be translated to detailed authentication requirements that can be satisfied through technical or operational solutions.

Transactions and data

Transactions

Transactions define the essential activities of a business or organization. They are the primary driver for analysis in the e-RA approach. To determine the best way to authenticate a specific group of users for a transaction, it is important to know the structure and contents of the transaction, who can use it, and what is expected to happen when it is used.

The transactions of a system are the specific actions that users can perform to get a desirable result. In other words a transaction is an actor, plus an action, resulting in a desired outcome. For example, a private citizen (actor) may inquire on government benefit programs (action) to learn about their eligibility (outcome).

Transaction data

Data is a valuable organizational asset. Depending on its purpose, data may be subject to security requirements such as confidentiality, integrity, and availability.

Transactions are an access path to data. They are the vehicle for creating data, inquiring on it, modifying it, or deleting it. Users utilize transactions to interface with data.

Unauthorized use of transactions permits unauthorized access to data, and potentially violates the data's security requirements. Transaction-based authentication is one control used to ensure that data, both individual and organizational, is protected from unauthorized actions. Considering the value of data accessed by transactions helps e-RA users to identify the risks of unauthorized use and to choose appropriate authentication levels.

Primary e-RA activities

Users perform four primary activities in the e-RA assessment:

- capture initiative information

- set risk tolerances for their initiative

- identify the transactions of their system or initiative

- analyze those transactions for risks related to unauthorized use in order to arrive at authentication levels

These activities are described in detail in sections 1 through 8 of this document.

After using e-RA, a system owner has a mapping of each transaction to an authentication level. These levels can then be used to develop detailed authentication requirements for transactions and to choose and implement technical and other operational solutions for authentication.

Purpose and Use of the e-RA Database

The e-RA Database is designed to help users to perform an e-RA. It captures the assessment data and authentication decisions of the initiative.

Using the database, initiatives can perform as many assessments as they like, each of which can be identified by assessment date. Over time, the database can house all of the assessments performed by an initiative and can be consulted for historical or comparison purposes.

A single person or an entire assessment team can use the database. They may print reports for review or distribution to team members, management, and other stakeholders. Keep in mind that the database is only a data repository and is not designed to perform analysis of the initiative's data.

See appendices A and B for more information on using the e-RA Database.

System Requirements

This database can be used with Microsoft Access versions 2000 and newer. Older versions of Microsoft Access (i.e., Access 98) will not be able to run this database.

The database as delivered is intended for stand-alone use, and should not be implemented in a file-sharing environment with concurrent users.

Because of the size of the input forms in the database, it is also highly recommended that you set your screen size setting in the Control Panel to no less than 1280 X 1024. This will ensure that you are able to see all relevant input fields and buttons on each form.

The e-RA database has a series of menus for ease of navigation. Before accessing the e-RA menu screens, you must accept the warranty language on the screen that appears when you start the e-RA database.

Image 1: e-RA warranty screen

- If you do not accept the warranty, your e-RA database session will terminate.

- To accept the warranty terms, select the button with text that states "I ACCEPT." Once you accept the warranty language, you will be directed to the e-RA Menus.

Image 2: e-RA Menus

The first e-RA menu has four initial choices. Select from

- o   Perform e-RA Activities

- o   View or Print e-RA Reports

- o   View or Edit e-RA Issues List

- o   Quit e-RA

When you select an activity on the first menu screen, you will be directed to another menu to navigate through the e-RA database.

⚠️ **Some menus continue on subsequent menu screens. Make sure to look for these additional screens where lists of items are continued on another menu.**

Each menu also provides you the ability to navigate back to the first menu or any previous menu.

Perform e-RA Activities

This selection directs you to another series of menu items that list all of the e-RA assessment activities. From this screen, you may enter directly into any e-RA activity. Each activity is listed separately and if selected takes the user directly to the input form for that activity.

The e-RA Activities Menu is split into two menu pages. To navigate from one page to another, choose these selections:

- "Continue e-RA activities . . ." or
- "Return to e-RA activities. . ."

View or Print e-RA Reports

Almost every activity in the e-RA process has a report associated with it. This selection directs you to a menu that lists all of the e-RA reports.

The e-RA Reports Menu provides direct access to any e-RA report. Each available report is listed separately. Once selected, the report will be presented on the user's screen. You can then print the report using the toolbar options.

The e-RA Reports Menu is split into two menu pages. To navigate from one page to another, choose the "More reports . . ." and the "Return to e-RA reports. . ." selections.

View or Edit Issues list

The e-RA database has a form for recording any issues, concerns, problems, and action items while performing an assessment. You may access this form directly by selecting this menu item.

Quitting e-RA

This selection will close the e-RA Database tool. When it closes, the tool will save your data and compact and repair. This will re-organize the data within the database for efficiency upon re-entry.

⚠️ **If you encounter any problems while entering data in the database, it is best to quit and restart the database so that the tool can make repairs.**

Using e-RA Activity Forms

These forms are used for the presentation, entry, and modification of the data collected throughout the e-RA assessment. You may access these forms directly from the e-RA Activities Menu. Or, you may begin with Activity 1 and move to the next activity form by clicking the "Go to Next Activity" button.

⚠️ **Forms are not designed to be printed. If you print a form, be aware that all of the records that have been previously entered in the form will print as well. If you have entered 300 records, all 300 forms will print. You should view and print e-RA reports rather than forms if you want a printed copy of data that you have entered**.

For new users of Access, more information on using forms and form components is available in Appendix A.

Data entry and modification

Data entry

Forms allow you to enter and modify data for your e-RA assessment. Once data is entered and saved, you can then use the buttons to navigate through this data and to modify it as necessary. You will begin the data entry process with the first form, "Initiative Description," and end with the checklist in "Next Steps."

Data Modification

Once you have entered data into the e-RA database, you have the ability to modify this information. Key points to know while modifying data are these:

- Use the navigation buttons to search for the data that you want to modify.

- Changes and deletions will modify or eliminate all associated data.

Inputs to e-RA

To get started with an e-RA assessment, you will need

- OMB authentication levels, currently available at http://www.cio.gov/eauthentication/ (current as of 08-13-03) or another set of authentication levels you wish to use

- knowledgeable participants

  Generally, 1-5 people perform e-RA. They must be able to describe the transactions of the initiative and to identify and analyze the consequences of unauthorized use. It may also be helpful if the participants have access to others in the initiative or the sponsoring organization to contribute to or validate some decisions and outputs of e-RA.

- initiative business case

- list of initiative transactions

- e-RA Database

Once you have assembled these, open the e-RA Database in Microsoft Access and begin.

1 e-RA Initiative Description

The purpose of this activity is to record the basic information about an initiative.

Background

Although the information here is not used directly in any subsequent step of e-RA, it provides context.

For more background information, see **Concepts** (below).

Important tips

Caution: Don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit this form.

Performing the activity

1. Record the initiative name.

2. Record the sub-initiative name, if applicable.

3. Select the category of initiative.

4. Describe the initiative.

5. Record the types of actors who will use the initiative.

6. Select points of entry where users can access the initiative.

7. Click on the "Add/Save" button to save your work. You will see a blank screen. You can enter another initiative or continue to step 9.

8. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

The initiative can then direct further attention to these issues after the e-RA assessment or as a part of a regular risk assessment activity performed on the initiative.

Concepts

The purpose of this activity is to elicit a brief description of the initiative's mission or business case and the status of the development effort, if known.

e-RA participants describe the core services to be provided through the initiative. Gather sufficient detail to describe the boundaries of the initiative's services. Concentrate on identifying the extent to which the business processes and the structure (i.e., application and technical infrastructure) of the initiative have been defined. If the initiative has not been completely defined, focus the remainder of the e-RA activities on the proposed definition of the business processes and transactions.

You do not gather specific transaction detail in this activity. Rather, capture a general sense of the initiative's core mission so that this can be used as the context going forward in the assessment.

2 e-RA Assessment Information

Purpose

The purpose of this activity is to document the assessment date and the participants who performed the assessment.

Background

The e-RA Database Tool distinguishes each assessment by date. You may perform more than one assessment on an initiative. As conditions change, this also allows you to go back and review or update prior assessments.

Important tips

Caution: If you delete an assessment date, all data associated with this date throughout the e-RA Database Tool will be deleted.

Performing the activity

1. Check the shaded boxes at the top of the database form to ensure that the name of the initiative (and sub-initiative, if applicable) is correct.

2. Fill in the date box.

3. List the participants' names, separated by commas.

4. Click on the "Add/Save an Assessment Date" button.

5. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

3 e-RA Risk-Tolerance Criteria

Purpose

The purpose of this activity is to set the risk-tolerance criteria for your initiative.

Background

The set of risk-tolerance criteria that you develop serves as a benchmark, specific to your organization, for measuring the impacts of unauthorized use of transactions.

For more background information, see **Concepts** (below).

Important tips

Always check the top portion of any database form you that are working in to see that you are on the correct assessment by date.

You may need input from others in your organization or initiative in order to develop meaningful risk tolerance criteria.

You will find two examples of criteria for your reference. One is in the form of a report. Click on the "Default Risk Tolerance" button to see and print this document. The other example is in a form that allows you to use the text if the examples are close to the criteria that you need. Click on the "Example Risk Tolerance" button to see this document.

Performing the activity

1. Check the shaded boxes at the top of the form to ensure that the name of the initiative (and sub-initiative, if applicable) is correct.

2. Select an impact area from the area labeled "Impact Area."

3. Review the example criteria provided in the e-RA Database Tool by clicking on the "Example Risk Tolerance" button above "Impact Area" and decide how to modify these criteria to suit your initiative.

4. Record your definitions for high, medium, and low for each impact area in the boxes provided.

5. Continue with the next impact area until you have defined criteria for each of the seven impact areas provided.

6. Click on the "Add/Save Criteria" button.

7. Click on the button labeled "Risk Tolerance Criteria" to see your definitions. You may also print this report.

8. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

Concepts

Impact

Risk-tolerance criteria are developed to provide a specific way to measure the extent to which the initiative is affected by the consequences of unauthorized use of a transaction. The effect on the organization is defined as an "impact."

Risk-tolerance criteria

Risk tolerance criteria are benchmarks or measures against which the organization can evaluate the impacts of unauthorized use of an initiative's transactions. The risk-tolerance criteria reflect the organization's specific tolerance for risks.

In the e-RA approach, the risk-tolerance criteria embody three principles:

1. Because each organization has different drivers, the risk-tolerance criteria for each organization may be different. In essence, the organization develops its own weighting factors to describe what is important, rather than accepting these factors from external parties.

2. Risk-tolerance criteria are important for determining the appropriate type and extent of authentication controls that would prevent the impacts related to the unauthorized use of transactions.

3. The risk-tolerance criteria allow an initiative to determine the relative severity of a particular impact and to identify those impacts that the organization most wants to avoid. The relative severity is a qualitative measurement, described as high, medium, or low. For example, the effects of a financial fraud resulting from unauthorized use of a transaction will vary depending on the organization. If the fraud results in a $10 million loss, this may be a high impact to one organization and a low impact to another. The risk tolerance criteria are organization-specific to allow for these variations.

Impact areas

Risk tolerance criteria can be categorized or arranged by the type of impact that they describe. These categories are referred to as impact areas. In the e-RA approach, seven standard impact areas are provided for which you develop risk tolerance criteria:

- confidence & reputation – impacts that adversely affect the reputation of the initiative or its external partners or customers

- health & safety – impacts that adversely affect the health, safety, or wellness of the initiative or its external partners or customers

- productivity & performance – impacts that adversely affect the initiative's productivity or performance or the usability of the initiative's services by customers

- administrative action – impacts that adversely affect the initiative by causing or resulting in the imposition of administrative actions

- regulatory and legislative compliance – impacts that adversely affect the initiative's ability to comply with regulations and legislative requirements

- finance – impacts that adversely affect the initiative's financial state or circumstances or the financial state or circumstances of the initiative's external partners or customers

- fines and legal penalties – impacts that adversely affect the initiative by causing or resulting in the imposition of fines or legal penalties

When the consequences of unauthorized use of transactions are realized by the organization, these impact areas can be used to measure the extent of the effect on the organization.

4 e-RA Transaction Identification

Purpose

The purpose of this activity is to identify the set of transactions that will be assessed using the e-RA approach.

Background

Transactions form the basis for the e-RA approach.

You may assess as many transactions as you like.

Some initiatives only assess a subset of transactions from their initiative. If you decide to use a subset, make sure they are a representative sample.

For more background information, see **Concepts** (below).

Important tips

Always check the top portion of any database form that you are working in to see that you are on the correct assessment by date.

Caution: If you delete a transaction, all data associated with this transaction throughout the e-RA Database Tool will be deleted.

You can select the "Transaction Summary" report button at any time to see all the transactions you have recorded so far. You may also print this report.

Caution: Don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit this form.

Performing the activity

1. Check the shaded boxes at the top of the form to ensure that the date and name of the initiative (and sub-initiative, if applicable) is correct.

2. Fill in the transaction name.

3. Select a transaction type.

4. Record a transaction description. Write as much as you like to be clear in describing the transaction.

5. Describe the data associated with this transaction. Note any special restrictions on this data or indicators of sensitivity. You may also indicate any security requirements associated with the data (confidentiality, integrity, or availability).

6. If this transaction requires non-repudiation, check the box next to the statement, "Transaction Requires Non Repudiation."

7. Check all the boxes that apply next to Transaction Actor labels.

8. Click on the "Add a Transaction" button. This will save the current transaction and provide a clean form to record additional transactions.

9. Click on the button labeled "Transaction Summary" to see a list of your transactions. You may also print this report.

10. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

Concepts

Transaction-based assessment

Transactions are the primary driver for analysis in the e-RA approach. To determine the best way to authenticate a specific group of users for a transaction, it is important to know the structure of the transaction, who can use it, and what is expected to happen when it is used.

The transactions in an e-government initiative define the specific activities that are desired to meet the initiative's goals and objectives. For example, the ability for a private citizen to inquire on benefit programs that fit their individual needs could be a primary objective of an online eligibility assistance initiative. This transaction is meant to be used by a specific group of users and the desired outcomes (i.e., a private citizen gets valuable information on government benefit programs) have been established.

For some initiatives, a complete set of transactions for the initiative will be analyzed. For others, the transactions will be a **representative set**. Identifying the appropriate transactions depends on a number of factors, including the business purpose of the initiative, the current or expected logical and physical designs for the initiative's systems, and the boundaries of the initiative.

Transactions to include in the assessment

Understanding the criticality, volume, and range of transactions that the initiative offers will help to define authentication needs. Pilots of e-RA demonstrated that five to seven transactions are sufficient to successfully define authentication needs. If you are using a subset of transactions to define authentication requirements, consider the categories below to help you decide how to choose which transactions to analyze.

- Critical transactions – those most relevant to the purpose or mission, or without which the initiative could not fulfill its primary objectives. These transactions reveal the core of the services provided by the initiative and are those that need the most scrutiny.

- Common transactions – transactions that are used most frequently. Because they are used often, these transactions provide a greater possibility of misuse. There may be some overlap between common and critical transactions.

- Unique transactions – those that are neither common nor ordinary and that may have a special purpose or distinctive users.

- Range of transactions – the range of transactions defines the upper and lower limits of the transactions in terms of what they allow users to do, and that all types of transactions are covered

Transaction types

The risk assessment techniques for identifying the consequences of unauthorized use of transactions are highly dependent on the transaction type. Thus, each transaction that is assessed in the e-RA approach must be categorized in one of four types: inquire, create, modify, or delete. Each of these types is described below.

- Inquire – this transaction allows the user to access data or information. The user makes a request for information and receives it. This information may be related to the user in some way (i.e., private) or can be general information (i.e., public.).

- Create – this transaction allows the user to put new data or information in a system. The user creates new data that does not currently exist. However, if existing information is available in a system and new information is appended, the "create" transaction is essentially a modification of existing data, and is covered by the "modify" transaction.

- Modify – this transaction allows the user to modify existing data or information in a system and save those changes. The original information may or may not be recoverable.

- Delete – this transaction allows the user to destroy or eliminate data or information so that it is no longer available for inquiry or modification. The elimination of data or information may be temporary (recoverable) or permanent (unrecoverable.)

There are variations on these categories and you may also have some unique variations to describe. For example, "approve" may be a transaction in which a request or voucher is approved by an appropriate party. In the e-RA approach, this transaction is a form of a "modify" transaction because it appends additional data to the existing record. In addition, a "cancel" transaction could be classified as a type of "delete" in which an action or approval is voided. The original request or authorization may still be kept for historical purposes. You must be sure to thoroughly analyze the action of the transaction to properly categorize it. This may require you to describe unique situations in sufficient detail to ensure proper categorization.

Transaction data

Transactions are the gateway to a system's data or information. Providing access to use a particular transaction essentially provides access to the transaction's data. Implementing authentication controls to ensure that transactions are used only by authorized users is one way to protect data from unauthorized access.

You must consider a transaction's data in order to identify risks associated with unauthorized use of a transaction. For example, a transaction that permits a user to inquire on public information or data may not result in any risk because the data or information does not specifically need to be protected. However, if the inquiry is on private data, many risks may result because of the potential unauthorized disclosure of private data.

For each transaction, you should specifically identify the data associated with the transaction. You should consider and document

- whether the data's use will be restricted only to certain actors or groups of actors

- if the data must be available for use by the actors for any critical timeframe

- if the data is private, sensitive, or otherwise requiring a high level of protection

You may also want to note if the data has any specific information security requirements such as confidentiality, integrity, or availability. If so, these requirements should be considered when identifying the consequences of unauthorized use of transactions that access this data.

Other transaction information

You may want to record other information on transactions when defining them if that information is relevant to authentication needs. For example

- the flow of transactions (for example, a "create" must precede an "approval")

- unusual aspects of a transaction (for example, a "delete" transaction doesn't actually remove a record)

- the expected volume of the transaction

- triggered transactions or activities that occur when the transaction being reviewed is executed

Transaction actors

In the e-RA approach, actors are defined as the potential users who are most likely (or are intended) to execute the initiative's transactions. Defining actors is important to understanding the intent of the transaction and for deriving the most effective authentication controls for the transaction.

Many types of actors could be defined for the e-government initiatives. The following are some examples:

- government employees – all current, active employees of the federal government exclusive of the Department of Defense (DoD)

- DoD military and civilian employees, except for government contractors

- all United States private citizens

- authorized agents of United States private citizens – legally identified persons acting on the behalf of a U.S. citizen, such as a legal guardian

- government contractors – any company or organization with a current, valid contract to provide goods or services to a government agency

- foreign citizens, governments, and companies – any citizen, government, or company of a foreign government that uses an initiative's services

Non-repudiation

Non-repudiation is sometimes referred to as a business requirement rather than a security requirement. Either way, it is relevant to authentication. Non-repudiation is the specific identification of a user as well as the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction.

.

5 e-RA Risk Identification

Purpose

The purpose of this activity is to identify the consequences of unauthorized use of transactions.

Background

The threat of unauthorized use plus the resulting consequence of that action pose a risk.

For more background information, see **Concepts** (below).

Important tips

Always check the top portion of any database form that you are working in to see that you are on the correct assessment by date.

You can select the "Risk Identification" report button at any time to see the consequences you have recorded and saved so far. You may also print this report.

You will perform risk identification activities on one transaction at a time on this form. You should periodically check to ensure that you are working on the intended transaction.

This form provides a single response block to record consequence statements. You can record as many consequence statements as necessary, but you should avoid combining them into a single response. Use a blank form for each consequence statement.

The e-RA Database Tool includes lists of questions and example answers to prompt you to think about the consequences of unauthorized use. It is highly recommended that you use these questions to elicit consequence statements. If you use these questions, you do not need to answer every question. Conversely, you may identify many consequences in response to a single question that is particularly relevant for you.

1. Check the shaded boxes at the top of the form to ensure that the date and name of the initiative (and sub-initiative, if applicable) is correct.

2. Check the Transaction Name and Transaction Type boxes to confirm that you are assessing the intended transaction.

3. Click on the button labeled "Consequence Questions" to get a list of questions to help you develop statements that describe the consequences of unauthorized use of the transaction. Click on the button labeled "Example Consequence Statements" to see examples. You may print these lists for reference.

4. Record each consequence statement separately in the white box labeled "Record Your Consequence Statement". Write as much as you like to express that consequence. Put only one consequence in this box.

5. Click on the button labeled "Add a Statement" to save that statement and get a blank form for the next statement.

6. Repeat steps 4 and 5 until you have recorded all the consequence statements for that transaction.

7. Click on the arrow buttons next to "Scroll to consider all transactions" to advance to the next transaction or move to prior transactions to revise.

8. Repeat steps 2 through 7 until you have recorded all of the consequence statements for each of your transactions.

9. Click on the button labeled "Risk Identification" to see a list of all your consequences. You may also print this report.

10. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

Consequences of Unauthorized Use

A primary objective of the e-RA approach is to identify the consequences of unauthorized use of transactions, and the authentication controls necessary to prevent these consequences. The threat of unauthorized use of a transaction and the potential consequences constitutes a risk for the initiative.

In the risk identification activity, you develop and document the consequences of unauthorized use for each transaction that you are assessing. This is performed by answering a series of questions that help you to draw out consequence statements depending on the type of transaction you are assessing. The type of transaction (i.e., inquire, etc.) is important for developing these consequence statements because each type affects data in different ways.

For example, when an authorized user inquires on a payroll record, the desired outcome is that the authorized user (the owner of the record or their authorized agent) is able to view this information. Conversely, when an unauthorized user executes this inquiry, undesired outcomes occur, such as disclosure of personal information to other than the owner of the information. These undesired outcomes from unauthorized use of transactions present potential consequences to the initiative.

Transaction types and consequences

Depending on the type of transaction, unauthorized use can result in many possible undesired outcomes and consequences to the initiative. This is because of the inherent effect that each transaction has on related data and information.

You should consider these effects when determining the consequences of unauthorized use of a transaction. For example:

- *Inquire* transactions generally provide access to view data. Unauthorized use can result in disclosure of data to users other than the owner of the data. If the data is confidential or personal, this can cause serious consequences for the initiative, the owner of the data, etc. You should consider what consequences result from this unauthorized disclosure.

- *Modify* transactions allow the modification of existing data. Unauthorized use can affect the integrity of the data and the ability to use the data for the purpose intended by the owner or other authorized users. Remember also that unauthorized modification of data also causes disclosure (i.e., the data is seen by an unauthorized user before they modify it). You should consider what consequences result when the integrity of the data is affected.

- *Delete* transactions allow data to be deleted temporarily or permanently. Unauthorized use causes the data to be unavailable to the owner and other authorized users. If the loss of data is temporary, you should consider what consequences result from having to recover or restore this data, and the inability to use it temporarily for the purposes intended. If the loss is permanent, you should consider what consequences result from the permanent inability to use this data for the purposes intended.

- *Create* transactions permit data to be recorded or documented. Unauthorized use can result in the creation of data that is misleading, fraudulent, or used for unintended purposes; essentially the integrity of existing data is put in question. The creation of unauthorized data can interfere with the use of existing data for authorized purposes. As with the unauthorized modification of data, you should consider what consequences result from the inability to use existing data for the purposes intended, or the use of data that may not be accurate.

Developing consequence statements

As you develop consequence statements, you need to consider the effects of unauthorized use as noted above. In addition, you should consider the consequence questions. These questions have been developed for each transaction type and prompt you to consider consequences as they relate to the various impact areas. (You were introduced to these areas when you developed your risk-tolerance criteria.) Thus, you develop consequence statements that reflect undesired outcomes and the effects on the initiative in areas such as reputation, health and safety, and finance.

Example of consequence statements

Composing effective consequence statements takes practice. Here is an example to guide your development of consequence statements: Consider a transaction that allows a user to inquire on a personal profile that they established to determine their eligibility for benefits. This profile contains significant personal data such as the user's social security number and any health conditions that they currently have, such as diabetes.

If an unauthorized user performs this transaction, the undesired outcome is a disclosure of private information to other than the owner of the information or their authorized agent. What are the resulting consequences of this unauthorized use?

To determine these consequences, we look to the consequence questions for transaction type "inquire." Consider the first question: What is the impact on the reputation of the initiative? This would result in the following consequence statement:

"The reputation of the initiative would be adversely affected. Users would not have confidence that we are adequately protecting users' personal data, and therefore they would stop using the web site. This would destroy our mission to bring government to the people."

Consider another question: What fines and regulatory issues would we be exposed to? By answering this question, another consequence statement is generated:

"Disclosing a user's private information would put the initiative in violation of the Privacy Act of 1963, and worse yet, would cause us to be out of compliance with HIPAA regulations. We would be fined $1,000, and probably be subjected to a Congressional Review or GAO audit."

Each of these consequence statements will play an important part in determining the appropriate level of authentication for transactions.

6 e-RA Risk Analysis

The purpose of this activity is to analyze the consequences of unauthorized use of transactions using the risk tolerance criteria for your initiative.

Background

Areas vital to achieving the organization's goals, objectives, and mission--such as reputation, customer confidence, finance, legal or regulatory, etc.--can be used to evaluate the consequences of unauthorized use.

When the consequences of unauthorized use are realized by the organization, these areas can be used to estimate the extent of the potential impact.

Important tips

Always check the top portion of any database form you are working in to see that you are on the correct assessment by date.

You may want to print the Risk-Tolerance Criteria Report to aid you in performing this activity. The report is available from the database form for activity 3 and from the e-RA menu; use the item labeled View or Print e-RA reports.

You can select "Risk Analysis" report button at any time to see the consequences and impact values you have recorded and saved so far in this activity. You may also print this report.

Performing the activity

Part 1 – Impact analysis

1. Check the shaded boxes at the top of the form to ensure that the date and name of the initiative (and sub-initiative, if applicable) is correct.

2. Check the Transaction Name and Transaction Type boxes to confirm that you are assessing the intended transaction.

3. Review each consequence statement and consider the extent of impact on the organization if this consequence is realized. Refer to your Risk-Tolerance Criteria to choose a value for the impact. Record this by selecting "high, medium, low, or N/A" values for each of the seven impact areas for each consequence.

4. Continue this activity for each consequence statement for a single transaction.

Part 2 – Choosing an authentication level

5. Select an appropriate authentication level for each consequence and set of impacts. Choose the level that would be most effective in preventing the consequence and resulting impacts from occurring.

6. Click on the arrow buttons next to "Scroll to consider all transactions" to advance to the next transaction or move to prior transactions to revise.

7. Repeat steps 2-6 until you have selected impact values and an authentication level for each consequence of all transactions.

8. Click on the button labeled "Risk Analysis" to see a list of your consequences and impact values. We recommend that you print this report or leave it open on your desktop to aid you in performing the next step.

9. Click on the "Go to Next Activity" button

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

Impact of unauthorized use

Even though consequences may result from unauthorized use of transactions, there may be no appreciable impact on the initiative. For example, if an unauthorized user inquires on public data or information, a consequence could be that the initiative is embarrassed because of a breach in security, but if that is only known internally to a few trusted insiders, there may be minimal overall impact on the initiative. However, if this becomes front page news in the *Washington Post*, the impact is much greater.

You developed the risk-tolerance criteria in Activity 3 so that you can measure the impact of consequences of unauthorized use of transactions specific to your initiative. If appearing on the front page of the *Washington Post* in a negative way is a particularly undesirable outcome for your initiative, you may consider this impact to be "high" based on your risk-tolerance criteria.

By determining the impact of a consequence, you are fully documenting the risk of unauthorized use of transactions for the initiative. Thus, risk is fully defined as the threat of unauthorized use, the consequences of realizing this threat, and the impact or extent to which the initiative is affected by these consequences.

Origin of authentication levels

For simplicity and consistency, authentication levels are used in e-RA to describe the various degrees of proving the identity of users. The developers of the e-RA approach have included authentication levels that are roughly based on UK standards and consistent with OMB standards. However, users of e-RA can substitute any authentication schema that works for them. The basic e-RA process is flexible and can be matched with a variety of authentication levels.

Purpose of authentication levels

In e-RA, the authentication levels have two primary purposes:

- to define the characteristics of authentication that a transaction would need to deploy to prevent risks of unauthorized use from being realized

- to provide a foundation for the development of detailed authentication requirements for a transaction that can be translated into technical requirements for implementation

It is important to note that the levels do not represent any particular authentication requirements or technical solutions.

In e-RA, the authentication levels are assigned first to the risks of unauthorized use for each transaction. Then, based on these authentication levels, an overall authentication level is assigned to the transaction.

Selecting authentication levels for each risk

The identification of risks provides further information regarding the extent to which the organization must develop and implement corresponding preventive controls (such as authentication) to mitigate the overall risk.

The first step in determining these authentication controls for a transaction is to determine the appropriate authentication levels for each risk that you have identified for each transaction. Thus, you should assign an authentication level for each risk (i.e., consequence statement and impacts) that you identified. These levels will help you in the next activity to determine an overall authentication level for a transaction.

To assign a level for each risk, you review each consequence statement and the impact values (that you have assigned to this statement) in each of the seven impact areas. This information is used to determine the authentication level that would prevent this consequence and resulting impacts from occurring. You perform this for every risk that you have identified for a transaction.

7 e-RA Transaction Authentication Levels

The purpose of this activity is to assign an authentication level to each transaction.

Background

At the transaction level, all of the risks (consequences of unauthorized use and their impact values) and their corresponding authentication levels must be considered to derive an authentication level for the transaction. There is no automatic process for doing this. It is a reasoning activity that requires the participants' knowledge and experience.

Important tips

Always check the top portion of any database form that you are working in to see that you are on the correct assessment by date.

You may want to print the Transaction Summary Report to aid you in performing this activity. The report is available from the database form for activity 4 and from the e-RA menu; use the item labeled View or Print e-RA reports.

Performing the activity

1. Check the shaded boxes at the top of the form to ensure that the date and name of the initiative (and sub-initiative, if applicable) is correct.

2. Review the authentication levels that you assigned to each of the risks (consequences and impacts) for each transaction.

3. Select an authentication level for the transaction.

4. Record any notes relevant to your selection.

For example, if you have assigned a "level two" to most of the transaction risks, but you have one "level three," you may still decide to assign "level three" to the overall transaction. You may record a note that indicates that the single "level three" risk is particularly undesirable and would need to be avoided, and therefore it is driving the overall transaction authentication level

5. Click on the button labeled "Transaction Level Summary" to see a summary of all your selections. You may also print this report.

6. Click on the "Go to Next Activity" button.

Other issues

At any time, you may click the button labeled "Record an Issue" to go to a form for capturing issues and concerns that arise during the assessment.

Concepts

Selecting authentication levels for each transaction

The final step in performing an e-RA assessment is to determine the authentication level that, based on risk, should be assigned to a transaction. There is no automatic means for doing this; it is an activity that requires the reasoning and knowledge of the initiative participants who are performing the assessment.

The basis for determining the transaction authentication level is the authentication levels you assigned to each transaction risk (consequence and impacts). You must look across these levels and resolve an overall level that is representative of all risks for the transaction. In some cases, this is simple—the authentication levels for each risk are the same, and therefore the transaction authentication level is the same. However, most often, you will have many different authentication levels assigned to individual risks for a transaction. To select an appropriate authentication level for a transaction, you must look at these levels and consider the risks to which they have been assigned.

For example, consider that you have 10 risks identified for a transaction, and you have assigned authentication levels as follows:

- two risks were assigned "level 1"

- three risks were assigned "level 2"

- four risks were assigned "level 3"

- one risk was assigned "level 4"

In this case, you might assume that the overall transaction should be assigned a "level 4." However, this may be cost prohibitive and you may decide that the majority of risks that you want to avoid are at "level 3." As a result, you assign a "level 3" to the transaction and decide to implement other types of controls to mitigate the one risk that required a "level 4." This is perfectly acceptable because you are making a risk-based decision, rather than a purely technical decision, which is in keeping with the underlying philosophy of the e-RA approach.

8 e-RA Next Steps

Background

You have completed e-RA. This form is provided as a convenience to help you with next steps.

Performing the activity

1. Review the checklist for possible actions.

2. Review and discuss anything you recorded in the Issues form.

3. Take action or record who will do the action and by what date.

4. Click on the button labeled "Go to e-RA Menu" to continue working on assessments or click on "Quit e-RA" to stop work.

More information

You may want to review the information developed, documented, and analyzed in the e-RA approach with other staff in the initiative (or other stakeholders) to ensure their understanding and agreement. This includes

- the risk-tolerance criteria used

- e-RA outputs, including the documentation of transactions, consequences, and their impact values

- the mapping of risks and transactions to authentication levels

- the other issues and concerns documented throughout the e-RA assessment

The value of discussing this information with the various stakeholders for the initiative is high. In these conversations, more information about the authentication needs of the initiative may be developed and considered. Important note: If you make changes to the risk-tolerance criteria based on these conversations, this can affect the analysis you performed in the process. You may need to go back and re-value the impacts of consequences. This might ultimately affect the mapping of risks and transactions to the authentication levels.

Remember that the authentication levels chosen for transactions may not entirely prevent the individual risks that you identified. In some cases, you will need to identify additional mitigation actions that are necessary (in addition to the authentication levels assigned to the transaction) to ensure proper preventive controls.

In addition, you may want to document detailed authentication requirements that are representative of the types of preventive controls that are necessary to ensure proper authentication. The authentication levels you assigned to transactions are a component of these requirements, but do not completely define the requirements.

Finally, the other issues and concerns identified throughout the e-RA activities need to be addressed. You may want to discuss these concerns with appropriate staff in the organization to determine if your concerns are legitimate, and whether any actions have been taken to mitigate them. You should develop mitigation strategies for those issues and concerns that you feel are not being addressed. You might also want to use this information as the basis for performing a more detailed risk assessment that covers the areas of risk to which an e-government initiative may be exposed.

Glossary

actors	The potential users who are most likely (or are intended) to execute the initiative's transactions, including government employees, DoD military and civilian employees, all United States private citizens, authorized agents of United States private citizens, government contractors, foreign citizens, governments, and companies.
authentication	One technique for identity management and access control; a way to ensure that users are who they say they are—that the user who attempts to perform functions in a system is in fact the user who is authorized to do so.
authentication levels	The authentication levels depict various aspects of user identity and authentication that a transaction might need to deploy. The levels are used in deciding the appropriate level of authentication necessary to mitigate or prevent risks identified during the e-RA approach. Developers of e-RA used the levels of authentication roughly based on the UK standards and consistent with forthcoming OMB standards. However, users of e-RA could substitute any authentication schema that works for them. The basic e-RA process is flexible and can be matched with a variety of authentication levels.
authentication levels	The characteristics of authentication that a transaction would need to prevent risks of unauthorized use from being realized. The foundation for the development of detailed authentication requirements for a transaction that can be translated into technical requirements for implementation.
authentication risk	Risk that could be avoided by appropriate authentication. The risks to which the initiative, its users, and its business partners would be subjected if unauthorized use of transactions occurs.
common transactions	Transactions that are used most frequently.
consequence statement	A description of the effects of unauthorized use of a transaction.
critical transactions	Transactions most relevant to the purpose or mission, or without which the initiative could not fulfill its primary objectives.
delete transaction	A transaction that allows the user to destroy or eliminate data or information so that it is no longer available for inquiry or modification. The elimination of data or information may be temporary (recoverable) or permanent (unrecoverable).

e-RA	The e-Authentication Risk and Requirements Assessment approach. It is a risk-based technique to elicit authentication requirements for transactions.
impact	The effect on the organization of a risk being realized; the effect of one thing on another.
impact area	Impacts categorized or arranged by the type of impact that they describe and used to measure the extent of the effect on the organization. Impact areas are confidence & reputation, health & safety, productivity & performance, administrative action, regulatory and legislative compliance, finance, and fines and legal penalties.
inquire transaction	A transaction that allows the user to access data or information. The user makes a request for information and receives it. This information may be related to the user in some way (i.e., private) or can be general information (i.e., public.).
modify transaction	A transaction that allows the user to modify existing data or information in a system and save those changes. The original information may or may not be recoverable.
non-repudiation	Specific identification of a user plus the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction.
range of transactions	A set that represents all the types of transactions. The upper and lower limits of the transactions in terms of what they allow users to do.
risk-based approach	The requirements elicited using e-RA are representative of, and derived from, the types of risks that the organization is trying to avoid.
risk-tolerance criteria	These criteria are benchmarks or measures against which the organization can evaluate the impacts of unauthorized use of an initiative's transactions. The risk assessment criteria reflect the organization's risk tolerances.
security requirements	Security requirements are the foundation of information security. They are: confidentiality, integrity, and availability. Authentication and non-repudiation are sometimes also characterized as security requirements. Security requirements embody many of the concepts important to the authentication process. Violations of security requirements as the result of unauthorized use of transactions and the resulting undesired outcomes directly affect the organization and are reflected in the types of impacts that can be identified.
transaction	The transactions of a system are the specific actions that users can perform to achieve a desirable result. A transaction is an actor, plus an action, resulting in an desired outcome.

transaction data	Transactions are the vehicle for creating system data, inquiring on it, modifying it, or deleting it. Authentication is one control used to ensure that data, both personal and organizational, is protected from unauthorized actions. Considering the value of data accessed by transactions helps e-RA users to realize the consequences of unauthorized use and choose appropriate authentication levels.
transaction levels	The authentication level for a transaction, considering all of the risks (consequences of unauthorized use and their impact values) and their corresponding authentication levels.
transaction types	Four types of transactions for web-based systems: create, delete, inquire, and modify.
unique transactions	Transactions that are neither common nor ordinary and that may have a special purpose or distinctive users.

Appendix A: Using Forms

There are eight basic activity forms in the e-RA Database:

- Activity 1: Initiative Description – record the basic information about an initiative

- Activity 2: Assessment Information – document the assessment date and the participants who performed the assessment

- Activity 3: Risk Tolerance Criteria – identify the tolerance for risk in your specific organization

- Activity 4: Transaction Identification – identify transactions that an initiative offers

- Activity 5: Risk Identification – identify the consequences of unauthorized use of the transactions

- Activity 6: Risk Analysis – apply the risk-tolerance criteria to the consequences of unauthorized use of transactions

- Activity 7: Transaction Authentication Levels – assign authentication levels to each transaction

- Activity 8: Next Steps – use checklist to reflect completion of the e-RA process and post-assessment activities

Image 3: e-RA form example

e-RA activity forms are composed of labels, fields, and buttons. Labels are made up of text that identifies specific information related to the form, such as sections or fields. The boxes, or fields, display the data stored in the database. Different fonts are used in the forms to differentiate between labels and data entered and stored in the database. Buttons allow you to navigate and perform actions in the form and entire database.

The forms are generally presented in zones. Each form has:

▪ a title in the upper left-hand corner

▪ a body consisting of all of the fields

▪ buttons along the right side

Shaded Fields

Many forms display shaded fields. The data displayed in these fields has already been entered in previous forms. Data in shaded fields cannot be changed unless you change it where it originates. For example, you cannot change an assessment date unless you do so in the Assessment Information form.

Shaded fields frequently include data about the initiative and the assessment date.

⚠ **You should refer to these fields frequently to ensure that you are working on the correct assessment.**

White Fields

White fields are used for data entry. They can capture data in several different formats. Those fields marked with an "(R)" are required. You must enter data into these fields to proceed.

Types of data-entry fields include date fields, text boxes, check boxes, and pull-down menu boxes.

- Text boxes allow free-form entry of data. There are no formatting restrictions. Whenever you exceed the visible space of the text box, a scroll bar will appear.

- Date fields accept a date in the format of a two-digit month and day, and a four-digit year (mm/dd/yyyy). As you type into this field, your data will automatically be formatted as noted.

- Check boxes are small white boxes with text in line next to them. You may select as many choices as are available on the form. A box appears as checked when you click in the white space of the box.

- Pull-down menus look like a text box, but have a button with a picture of an arrow on it in the right side of the box. When you click on this arrow, a menu appears with a number of choices. Select the appropriate choice by dragging your mouse down the list and clicking on your selection.

Buttons

Buttons are generally displayed along the right side of a form. They are divided into sections that are labeled with their actions. Buttons allow you to navigate and perform certain actions in the form and in the entire database.

Form navigation

You may navigate the e-RA forms by using your mouse, <Tab> key, <Enter> key or arrow keys.

Tab order

Tab order on the e-RA database forms has been predefined based on ease of data entry. Upon opening a form, the cursor will be positioned in the first available field where you are able to enter data. When you have completed a field, you can move to the next field by

- pressing the <Tab> key or

- positioning your mouse to click in the next box or

- pressing the <Enter> key

You cannot tab through check box lists and buttons. To access these boxes and buttons, you must position your mouse on them.

If you tab through all of the white fields on a form, you will advance to a new clean form.

⚠ **Be cautious — don't advance through the white fields until you have entered data in the check boxes. Otherwise, you will have to go back and edit the previous form.**
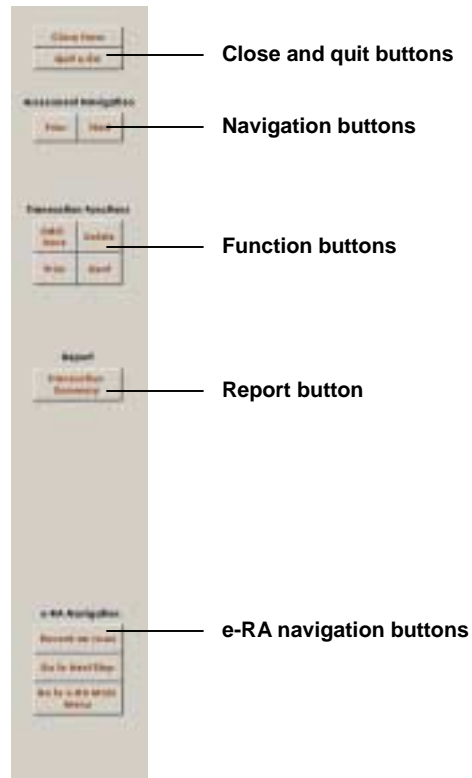
Buttons

Image 4: Form button examples

Form buttons are clustered and positioned close to the data that they pertain to. They perform the following actions:

- open a form
- close a form
- quit the database
- add or save data
- delete data
- move to the prior record in the database
- move to the next record in the database
- open a report
- go to the e-RA Menu

Close and quit

The buttons in the upper right-hand corner of every form will close the form or quit the e-RA database.

⚠ **Caution: If you quit the e-RA database, there is a chance that the data you have entered on the form will not be saved. You must click "Add/Save" before you choose "Quit e-RA" on forms where an Add/Save button appears.**

Function buttons

Function buttons relate to the core of the data that is being entered for a specific e-RA activity. For example, if you are entering data into the Transactions form, the function buttons indicate example transactions, add/delete a transaction, and view next and prior transactions.

On each form where these buttons appear, they perform the same basic functions:

▪ Add/Save – this is a dual-purpose button. When pressed, it will save the data you have entered and advance to a blank form. It is suggested that you save often. However, note that if you add/save before you have completed the entire form, you will need to return to the form later to complete the remaining fields.

▪ Delete – this button will not only delete the information entered in the form where the cursor is located, but all information related to that data. For example, if you delete an assessment date, all e-RA information associated with that date will also be deleted. You will receive a warning when you initiate this action, when a warning is applicable.

▪ Prior and Next – these buttons allow you to move back and forth between data that you have entered.

Assessment navigation

The assessment date is the primary identifier for storing information in the e-RA database and affects navigation. As you enter data on the forms, you must check the top of the form to ensure that you are working on the correct assessment. Navigation buttons have arrows on them.

The assessment navigation buttons allow you to move back and forth among all of the assessments that you have performed. If you only have one assessment, these buttons are moot. However, if you would like to review data from a previous assessment, use the button with the red arrow pointing to the right pictured on it to go back to a previous assessment and then the button with the red arrow pointing to the left to return to the current assessment.

e-RA Navigation

The e-RA navigation buttons allow you to go to other areas of the database. They perform the following functions:

- "Record an Issue" – opens the "Issues and Concerns" form.

- "Go to Prior Activity" – opens the previous activity form in the e-RA assessment and closes the current form.

- "Go to Next Activity" – opens the next activity form in the e-RA assessment and closes the current form.

- "Go to e-RA Menu" – takes you to the e-RA menu and closes the current form.

Other buttons

There are also a few unique buttons that appear on some forms. Some of these buttons uniquely describe the action that will occur upon a click. Common actions of these unique buttons are

- add the current record

- delete the current record

- view the prior records entered in the database

- view the next records stored in the database

- provide examples – for example, a list of transaction statements from a button on the Transaction Identification form

- offer guidance – on the Risk Identification form, a button will open a list of questions that will aid in your determination of consequences of unauthorized use of a transaction; the list of questions varies according to the type of transaction that you are examining

- scroll through previously entered data

- bring up a report that displays the information entered on the form

⚠ **Saving data in a form—no data is saved in a form until you have tabbed through all fields to a blank form, or pressed the "Add/Save" button.**

Appendix B: Viewing Assessment Reports

Nine database reports present the data collected in the e-RA process. These reports will allow you to distribute information and check your work. They are titled

- Initiative Information

- Initiative Risk-Tolerance Criteria

- Default Risk-Tolerance Criteria

- Transaction Summary

- Risk Identification

- Risk Analysis

- Transaction-Level Summary

- Issues

- Next Steps

Report presentation

Printing all of the reports will give you a complete picture of all of your initiative information or a specific assessment. Through reports, the e-RA database gives you the opportunity to view all recorded data. From there, you may review, distribute, and check your information.

Each report summarizes information for each activity in the e-RA process. Reports will only display data that has been properly saved in the database. You may generate reports by clicking on a report button from the e-RA Menu or on any form within the database. When you click on a button to see a report, some reports display a box that prompts the user for an assessment date. The message in this box reads, "Enter an Assessment Date (OK for all Dates)." At this point, you have two options:

- Type in an assessment date to view data collected for a specific assessment. Use the format of a two-digit month and day, and a four-digit year (mm/dd/yyyy).

- Press the <Enter> key on your keyboard to view the data for all assessments.
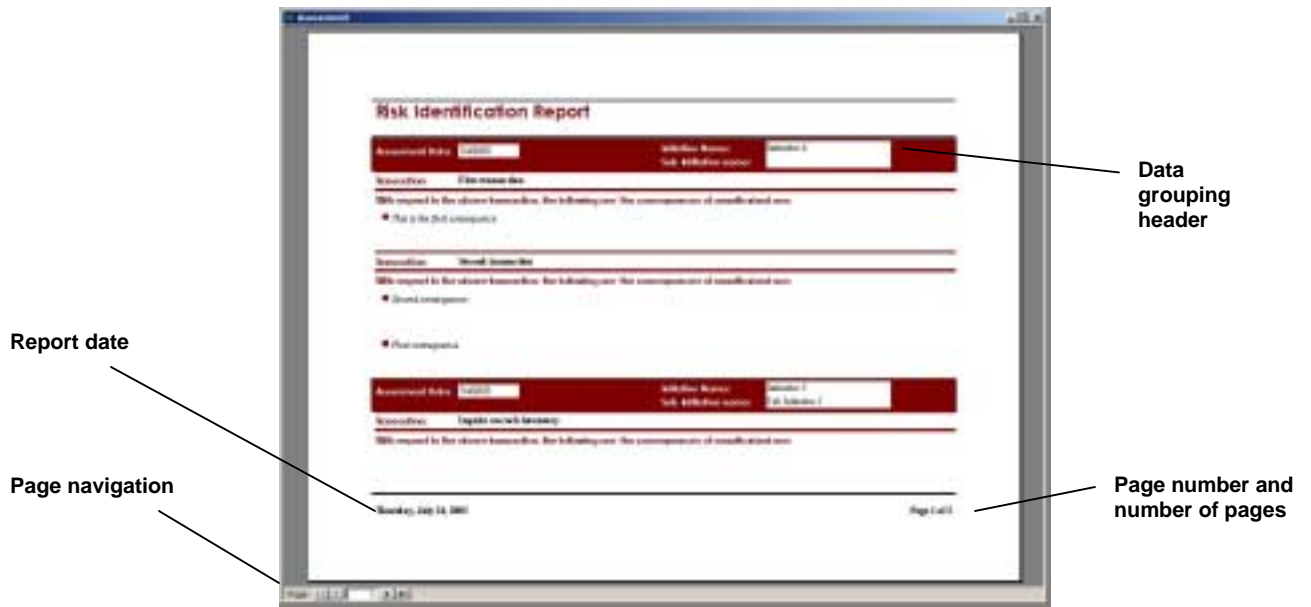

Image 5: Report example

Report features include these:

- The date that the report is generated is in the lower left-hand corner.

- A page navigation button is below the date in the lower left-hand corner of the sheet.

- Page numbers and the number of pages are in the lower right-hand corner of the sheet.

- Reports will group and sort on specific data.

To close a report, click on the "X" in the upper right-hand corner of the box that the report is in.

⚠ **If the report is being viewed full-screen, you must minimize the report screen before closing it.**

We have illustrated the various reports below and have outlined specific information about each.

Initiative and Assessment Description

This report is used to report on both Activities 1 and 2 and displays the following information:

- Initiative Name

- Sub-Initiative Name

- Initiative Description

- Initiative Actors

- Initiative Category

- Initiative Entry Points

- Initiative Assessment Date – listed with participants next to each date

- Participants – for each assessment date

Initiative Risk-Tolerance Criteria

This report shows the data recorded in Activity 3:

- Initiative Name – grouping the information below

- Sub-initiative Name – along with the Initiative name, form the overall heading and act as separator of the information

- Impact Areas – listed along the left-hand side of the report

- High, Medium, and Low criteria – decided by the organization performing e-RA for each impact area

Default Risk-Tolerance Criteria

You may use this report as a reference as you develop the Risk-Tolerance Criteria for your initiative in Activity 3. This report shows general high, medium, and low criteria for each impact area.

Transaction Summary

The Transaction Summary report provides information regarding all transactions for a particular assessment date. Use this report to show the data that you entered in Activity 4. This report will show the following information:

- Initiative Name

- Sub-Initiative Name

- Assessment Date

- Transaction Name

- Transaction Type

- Transaction Description

- Transaction Data

- Non-Repudiation – check box

- Other Information – recorded about the transaction

- Transaction Actors

Risk Identification

This report lists the consequence statements for each transaction recorded in one assessment.

Consequence Questions

Use this report as a reference while completing Activity 5: Risk Identification. In this exercise, you describe the consequences of unauthorized use of a transaction by transaction type. This report will show the comprehensive list of questions for each type of transaction.

Risk Analysis

Use this report with Activity 6, in which you record the values for each consequence statement in an assessment. The following information will be on this report:

- Assessment Date

- Initiative Name

- Sub-Initiative Name

- Transaction Name

- Transaction Authentication Level – this item is added to the report after Activity 7

- Consequence Statements – for each transaction

- Impact Values in Reputation, Health, Productivity, Administrative, Regulatory, Finance, and Fines – these are lined up with the consequence statements on the report

- Consequence Authentication Level – for each consequence statement

Transaction Level Summary

This report lists the transactions for each assessment and their corresponding transaction levels. You choose these transaction levels in Activity 7.

Next Steps Checklist

This report will capture any next steps in an assessment. It is in a checklist format as it is on the Activity 8 form.

Issues

This report has the list of issues that you recorded while going through the e-RA process. This report also shows the Issue Category and Mitigation that you documented for each issue.